Computer Security Weaknesses at State Agencies Put Federal Tax Information at Risk

February 2003

Reference Number: 2003-20-064

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

February 21, 2003

MEMORANDUM FOR CHIEF, COMMUNICATIONS AND LIAISON

FROM: Gordon C. Milbourn III
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Computer Security Weaknesses at State Agencies Put Federal Tax Information at Risk
(Audit # 200220024)

This report presents the results of our review of the security of computerized federal tax data maintained by state governments. The Internal Revenue Code[1] requires the Internal Revenue Service (IRS) to disclose federal tax information to various state and federal agencies. According to IRS records, federal tax information is provided to over 250 state and federal agencies. To protect taxpayer privacy, these agencies are required to protect sensitive data, and the IRS is required to periodically review the agencies' controls.

In summary, we concluded that computerized federal tax information is at risk while in the possession of state agencies. We noted weaknesses at the states' Internet gateways that could be exploited by hackers and disgruntled employees. Unencrypted data was being transmitted between sites, controls were not always adequate to authenticate users, and activity logs (audit trails) were not always used to detect improper activity. Some states did not proactively monitor system activity to identify inappropriate browsing of taxpayers' accounts.

State governments are primarily responsible for protecting tax data received from the IRS and risk losing access to that data if they do not provide adequate security. For this review, we did not attempt to identify the root cause of the weaknesses at each state agency. Instead, we focused on what the IRS needs to do to ensure that weaknesses are identified and corrected.

The IRS' Office of Governmental Liaison and Disclosure (GLD) conducted reviews of state agencies and, when weaknesses were identified, followed up to ensure they were corrected. However, the computer security portions of the reviews were generally

[1] Internal Revenue Code (I.R.C.) § 6103.

focused on mainframe computer controls. Since government computers are usually connected via internal networks and the Internet, data can be accessed from virtually any computer with an Internet address, not just the computer in which data are stored and processed. Appropriate security controls at Internet gateways and internally networked computers are equally important to reduce the risk that unauthorized users can access or manipulate taxpayer data.

The GLD does not have the technical expertise on staff to conduct full-scope security reviews and has had difficulty obtaining qualified assistance from other units in the IRS. Staffing is further complicated by the need to have technical skills available to evaluate the different computers and operating systems used by the federal and state agencies. Assigning sufficient and competent staff to these reviews is critical.

Because of the large number of state and federal agencies receiving federal tax data and the many different types of computers and operating systems they use, we recommended that the IRS broaden the scope of the GLD's reviews to incorporate other significant security issues, not just mainframe security, and require state agencies to conduct annual self-assessments using the guide provided by the National Institute of Standards and Technology (NIST). All federal agencies are required to use this guide in assessing their own systems. The self-assessments would allow the GLD to better focus the scope of its reviews. In addition, the GLD needs to hire additional staff, train and develop existing staff, or contract with outside consultants to conduct the necessary reviews.

Management's Response: The Chief, Communications and Liaison, agreed with the recommendations in this report and stated that this is an area that warrants increased attention. Corrective actions include increasing the scope of computer security reviews to include peripheral devices and exploring using the NIST self-assessment review guide or an equivalent to conduct the reviews. In addition, the GLD is conducting a study to assess alternatives such as hiring additional staff or contracting with professional security consultants to carry out the necessary reviews. Management is also determining the feasibility of self-certification and conducting joint audits with other federal agencies. Finally, management is conducting risk assessment studies so that future reviews focus on the areas of greatest risk. Management's complete response to the draft report is included as Appendix IV.

Copies of this report are also being sent to the IRS managers who are affected by the report. Please contact me at (202) 622-6510 if you have questions or Gary V. Hinkle, Acting Assistant Inspector General for Audit (Information Systems Programs), at (202) 927-7291.

Table of Contents

Background

Internal Revenue Code (I.R.C.) § 6103 requires the Internal Revenue Service (IRS) to disclose federal tax information to various state and federal agencies. State tax agencies can use this information to identify nonfilers of state tax returns, determine discrepancies in the reporting of income, locate delinquent taxpayers, and determine whether IRS adjustments have state tax consequences.

As a condition of receiving federal tax information, state tax agencies must have physical and computer system safeguards designed to prevent unauthorized accesses and use of this information. Due to the volume of computerized information the IRS provides to state tax agencies, safeguards to protect computerized information and the systems that process this information become critical.

Before a state tax agency receives federal tax information, it must submit to the IRS for approval a Safeguard Procedures Report (SPR) that describes how the state will protect and safeguard federal tax information. Agencies are requested to submit a new SPR every 6 years or whenever significant changes occur in their Safeguard Program. Agencies are required to annually file a Safeguard Activity Report to report minor changes to their safeguard procedures, advise the IRS of future actions that will affect safeguard procedures, and certify that they are protecting taxpayer information.

The Office of Governmental Liaison and Disclosure (GLD), within the Communications and Liaison Division, has primary responsibility for programs that provide federal tax information to state tax agencies. The GLD is responsible for ensuring that state tax agencies properly safeguard federal tax information. To do this, it is required to review and approve Safeguard Procedures and Safeguard Activity Reports submitted by state tax agencies and conduct on-site Safeguard Reviews of each state tax agency at least once every 3 years.

The audit was conducted between May and October 2002 at the GLD in the IRS National Headquarters. We also visited and reviewed security at five state tax agencies that receive federal tax information and met with GLD Disclosure Officers assigned to those state agencies. We reviewed

Safeguard Review Reports from 13 state tax agencies. The audit was conducted in accordance with *Government Auditing Standards.* Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

We did not review the security of the data being shared with non-tax state agencies or federal agencies. Controls to prevent the disclosure of taxpayer information by these agencies were evaluated in another recent Treasury Inspector General for Tax Administration report.[1]

State Governments Had Significant Computer Security Weaknesses That Jeopardized Federal Tax Information

In each of the five states we reviewed, federal tax information was delivered to the state tax agency reasonably secured. Any subsequent transmissions or deliveries within the state tax agency were also accomplished in a reasonably secure manner. In addition, physical security controls were generally adequate.

However, state governments' computer systems did not adequately protect federal tax information. Hackers and unscrupulous state government employees could have exploited security weaknesses to gain unauthorized access to federal tax information. Some of the more significant weaknesses identified in at least one office follow:

- Passwords for accessing the mainframe computer containing federal tax information were being sent unencrypted over telecommunication lines. Tools are readily available to hackers interested in intercepting passwords that could then be used to access sensitive data.
- The Internet router being used was outdated and did not contain the latest security patches. Router security weaknesses are well known by the hacker community and can be exploited to gain access to sensitive data through the Internet.

[1] *Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information* (Reference Number 2003-40-022, dated December 2002).

- Three individuals shared the password to the firewall administrator's account. Consequently, accountability for any inappropriate actions would not be determinable.
- Intrusion detection systems had not been implemented to detect hackers attempting to access their systems.
- Access to the mainframe computer was allowed through an excessive number of ports. The more ports left open by administrators, the more paths hackers could take in accessing sensitive data.
- Activity logs (audit trails) were not run or reviewed to identify inappropriate accesses. For example, few security and auditing functions were enabled on the network audit trails, and the logs on the Internet router were being routinely overwritten before being saved. Also, failed logon attempts (which could be an indication of unauthorized users trying to guess their way into the system) were not being recorded.
- Access to a server was not limited to authenticated users with valid logons and passwords.
- The proximity card system was not periodically queried to determine if any employees had access to areas that they rarely or never used, which might indicate they no longer need such access. However, proper procedures were in place for issuing proximity cards to control physical access to selected work areas. At one state, these procedures appropriately included revising access as employees' duties changed, deleting access when employees terminated, and frequently checking that personnel actions procedures were operating as intended.

In addition, two states had no proactive monitoring of audit trails for detecting inappropriate browsing. Potential unauthorized accesses were not flagged, so such instances would be identified and investigated only as the result of a complaint. State agencies receiving federal tax information

are bound by the same laws as the IRS regarding browsing taxpayer accounts for personal reasons.[2]

States are primarily responsible for the security of tax data received from the IRS and risk losing access to the data if they do not provide adequate security. For this review, we did not attempt to determine the root causes for the problems in the states. Instead, we focused on what the IRS needs to do to ensure that state governments protect federal tax information.

The GLD performed the required reviews of state computer system security. When weaknesses had been identified on prior reviews, disclosure officers followed up to ensure they had been corrected. However, the reviews conducted were generally not sufficient in scope to provide assurance that the states had adequate controls to protect sensitive taxpayer data. In particular, the GLD did not adequately assess key computer security issues in the 13 Safeguard Reviews we reviewed.

In 3 of the 13 reviews, the Disclosure Officers could not obtain assistance from an IRS computer security analyst to perform the computer security portion of the safeguard review. In these cases, the review consisted of the Disclosure Officers either reviewing answers to a questionnaire completed by state personnel or discussing computer security policies and procedures with state personnel.

In 7 of the other 10 reviews, the GLD focused its reviews on the mainframe computers containing IRS data. Computer security analysts believed that the mainframe controls were the most significant, since the primary data resided there. Some of the mainframe controls reviewed by the GLD included controls for identifying and authenticating users, restricting the computer resources users can access, tracking certain activities and accesses performed by users, erasing taxpayer data when no longer needed, providing system documentation and manuals, and protecting password files.

---

[2] Taxpayer Browsing Protection Act, 26 U.S.C. § § 7213, 7213A, 7431 (1994 & Supp. IV 1998).

The GLD's scope went beyond the mainframe and included network security in 3 of the 10 reviews. None of the 13 reviews included using a vulnerability assessment scanner for testing computers and other network devices for vulnerabilities.

Generally, the following significant security issues were not addressed by the GLD:

- Internet gateways and firewalls.
- Intrusion detection systems.
- Network servers and network security.
- Methods for securely transmitting tax information in e-mail transmissions.
- Remote access security.
- Installation of vendor software security patches.
- Testing states' computer systems and network security, including vulnerability scanning, penetration testing, password cracking, or social engineering.

In today's environment where computers are connected to internal networks and to the Internet, data can be accessed from virtually any computer with an Internet address, not just the computer in which data are stored and processed. Security controls at Internet gateways, web servers, e-mail servers, and remote access servers, are at least as important as security on mainframe computers to ensure that data cannot be accessed or manipulated by unauthorized persons.

Due to the large number of state and federal agencies receiving federal tax information, and the wide variance in the computers and operating systems used by those agencies, expanding the scope of the current reviews is a challenge. The GLD has been actively engaged in addressing these issues. In the last year, it has hired an expert security review team to develop review standards for different operating systems, explored self-certification and third-party certification, and obtained agreement from the states to cooperate in developing a better review process.

The GLD has not assigned sufficient, qualified staff to review computer security

According to IRS records, the GLD is charged with evaluating the computer security of over 250 federal and state agencies that have been provided federal tax information. Reviews are required at least once every 3 years, thus an average of over 80 reviews need to be conducted annually.

Assigning sufficient and competent staff to these reviews is critical. Staffing is further complicated by the need to have technical skills available to evaluate the different computers and operating systems used by the federal and state agencies.

The GLD did not have the technical expertise on staff to conduct full-scope security reviews. The GLD only had two security analysts assigned to assist Disclosure Officers with the computer security portion of the Safeguard Review. As a result, Disclosure Officers generally developed their own contacts with computer security analysts in the Area Offices under the IRS' Information Technology Services (ITS) organization to obtain assistance, if they were available.

In 3 of the 13 Safeguard Reviews we evaluated, the education, experience, and training of the computer security analysts conducting the security reviews were not broad enough to adequately test all areas of computer security. Further, as previously stated, in three other cases computer security analysts were not available to assist in the review. As a result, the IRS did not have adequate assurance that the states were protecting federal tax data.

The GLD had engaged an outside computer consultant to assist in the preparation of safeguard review guidelines and to conduct several reviews at state agencies. GLD management advised us that they were assessing the results of that work and will decide the future extent of the consultant's involvement in the safeguard review process.

Recommendations

Several alternatives are available to address the issues in this report. We recommend that the Director, GLD:

1. Broaden the scope of the GLD's reviews to incorporate other significant security issues, not just mainframe security. We suggest that the GLD require all state agencies to use the self-assessment review guide developed by the National Institute of Standards and Technology (NIST) that all federal agencies are required to use. The guide is applicable to all computers and systems containing sensitive data. It clearly outlines key security issues and guides users to determine whether policies and procedures have been developed, implemented, and tested. States should be required to submit these self-assessments annually with their Safeguard Activity Reports. The GLD could then use the self-assessments to focus the scope of its reviews.

Management's Response: Management agreed with this recommendation and will expand the scope of review to include peripheral devices. The GLD will also explore using the NIST self-assessment review guide or other appropriate equivalent.

2. Hire or develop an adequate number of employees to conduct the reviews. These specialists should have the background, education, and previous experience in computer security that will enable them, collectively, to comprehensively review the full range of computer systems used by state agencies. Hiring or developing these skills is difficult. As an alternative, consideration could be given to contracting with professional security consultants to carry out the necessary reviews.

Management's Response: Management agreed with this recommendation and is conducting a study to determine whether to hire additional staff or contract with professional security consultants to carry out the necessary reviews. In addition, management is looking into the feasibility of self-certification and conducting joint audits with other federal agency reviewers. Finally, the GLD is performing risk

assessment studies so that future reviews focus on the areas of greatest risk.

Appendix I

Detailed Objective, Scope, and Methodology

The objective of this audit was to evaluate the security of computerized federal tax data maintained by state governments.

To accomplish this objective, we:

I. Reviewed the status of the Safeguard Program using data on state agencies from the Office of Governmental Liaison and Disclosure (GLD) management information system.

II. Visited five state tax agencies to review physical and computer security of federal taxpayer information.

   A. Reviewed the states' physical security over computerized federal taxpayer information.

   B. Reviewed logical access controls over access to federal taxpayer information.

   C. Determined whether the states used audit trails to detect improper accesses to computers used to process or store federal taxpayer information. Determined if audit trails were turned on and reviewed on a regular basis.

   D. Determined whether the states used firewalls to prevent improper access to computers that process and store federal taxpayer information.

   E. Determined if an intrusion detection system was used to continuously monitor systems that process or store federal taxpayer information.

   F. Determined the extent to which the states self-review their systems.

III. Reviewed coverage given to computer security during safeguard reviews.

   A. Obtained and reviewed procedures and guidelines used by reviewers and computer security specialists for performing safeguard reviews and for performing the computer security portion of safeguard reviews.

   B. Reviewed the coverage given to computer security during safeguard reviews. Obtained documentation on Safeguard Reviews for 13 state tax agencies. The selected states consisted of the five states we visited and eight others. We judgmentally selected five small states, four medium states, and four large states in terms of the number of taxpayers residing in the state and the amount of computerized information they received from the GLD.

IV. Reviewed the qualification of IRS staff performing the computer security part of safeguard reviews.

V. Reviewed the GLD's monitoring of corrective actions.

A. Determined whether any state tax agencies had ever been suspended or terminated from receiving federal taxpayer information and, if so, whether it was because of computer security weaknesses.

B. Determined how the GLD ensured that state tax agencies implemented meaningful and timely corrective actions to computer security deficiencies in safeguard reports.

VI. Determined incidents of unauthorized access and disclosures. Determined whether there had been incidents in which state computer systems were used to make unauthorized accesses or disclosures of federal taxpayer information and, if so, the action taken by the GLD.

Appendix II

Major Contributors to This Report

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs)
Gary V. Hinkle, Acting Assistant Inspector General for Audit (Information Systems Programs)
Stephen R. Mullins, Director
Gerald H. Horn, Audit Manager
Dan Ardeleano, Senior Auditor
Richard T. Borst, Senior Auditor
Bret D. Hunter, Senior Auditor
Midori Ohno, Senior Auditor
Larry W. Reimer, Senior Auditor
Ted Tomko, Senior Auditor
Esther M. Wilson, Senior Auditor
James P. McCormick, Auditor

Appendix III

Report Distribution List

Acting Commissioner N:C
Director, Office of Governmental Liaison and Disclosure CL:GLD
Director, Disclosure CL:GLD:D
Chief, Security Services M:S
Chief Counsel CC
National Taxpayer Advocate TA
Director, Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis N:ADC:R:O
Office of Management Controls N:CFO:F:M
Audit Liaison: Office of Security Services M:S

Appendix IV

Management's Response to the Draft Report

CHIEF COMMUNICATIONS
AND LIAISON

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

RECEIVED
FEB 12 2003

February 12, 2003

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: David R. Williams
Chief, Communications and Liaison

SUBJECT: Management Response to Audit Report #200220024
Computer Security Weaknesses at State Agencies Put
Federal Tax Information at Risk

Your report on information security at state agencies will help guide our ongoing efforts to ensure that the states are properly protecting federal tax information (FTI). I agree that this is an area that warrants increased attention. To this end, I have devoted considerable resources to improve IRS' approach to protecting federal tax information through the monitoring of states' information security activities.

During the last 18 months, we:

- Developed new business processes and procedures to ensure we guide the states in their information security activities.
- Hired computer security experts to develop evaluation criteria that applies IRS information security standards to the multiple and diverse state computer platforms now in operation.
- Ensured the computer security experts train and assist IRS staff in conducting reviews and in applying the newly developed information security standards.
- Established performance measures to better monitor the timeliness, accuracy and completeness of the safeguard reviews.

I agree that despite these efforts, the IRS is struggling with the proliferation of increasingly sophisticated computer systems coupled with the lack of adequate staff expertise. In your report you recommend that the IRS hire additional staff to address this problem. However, the sheer number and diversity of state computer systems make hiring and retaining a staff fluent in information security standards impracticable.

Therefore, while we are exploring your recommendation as an alternative, we are also considering different approaches, such as third-party or self-certification. In addition we are conducting several risk assessment studies so that future reviews can focus on the areas of greatest risk. We would welcome any thoughts or suggestions you might have in regard to possible alternatives.

In conclusion, we believe we are making progress in improving our program. However, we also recognize that we still have a long way to go before we can be fully satisfied with our Safeguard program. Thank you for your recommendations. I have attached a detailed response outlining the corrective actions IRS plans to take to address your findings and recommendations.

Recommendation 1
Broaden the scope of the Governmental Liaison and Disclosure's (GLD) reviews to incorporate other significant security issues, not just mainframe security. Due to the large number of state and federal agencies receiving federal tax information, and the wide variance in the computers and operating systems used by those agencies, expanding the scope of the current reviews is a challenge. We suggest that the GLD require all state agencies to use the self-assessment review guide developed by the National Institute of Standards and Technology that all federal agencies are required to use. This guide is applicable to all computers and systems containing sensitive data It clearly outlines key security issues and guides users to determine whether policies and procedures have been developed, implemented, and tested. States should be required to submit these self-assessments annually with their Safeguard Activity Reports. The GLD could then use the self-assessments to focus its reviews.

Assessment of Cause
A state agency must provide numerous assurances to the IRS before FTI is released to it. This is commonly referred to as the Safeguard Program. The Safeguard Program elements include Memorandums of Understanding that clearly describe what is expected of the states; educational outreach activities designed to reinforce the requirement and provide some level of guidance; a detailed report from the agency that describes how they plan to protect the information; an on-site visit by the IRS; an annual notification from the states certifying that they are protecting the information; an annual Need and Use Review to verify that the information is still needed; and finally, an on-site Safeguard Review the agency performs every three years. It is the Safeguard Review portion of the program that is at issue here.

The proliferation of computer systems among the states poses an enormous challenge for the IRS. While the IRS has clearly articulated to the states their responsibility to protect FTI both in the physical and computer environment our ability to monitor the technology portion of their security measures is limited. We are working to enhance mainframe security but recognize we still need to develop capabilities to consider peripherals such as routers, switches and hubs.

Corrective Action
We agree with your recommendation to expand the scope of the reviews. As we enhance our ability to perform computer security reviews and develop risk assessment tools, we will also incorporate reviews of peripheral devices as well. In addition, we will explore using the National Institute of Standards and Technology self-assessment review guide or an equivalent that might be more appropriate for the states.

Implementation Date
Proposed Date: December 31, 2003

Responsible Official
Deputy Director, Governmental Liaison and Disclosure

Recommendation 2
Hire or develop an adequate number of employees to conduct the reviews. These specialists should have the background, education, and previous experience in computer security that will enable them, collectively, to comprehensively review the full range of computer systems used by state agencies. Hiring or developing these skills is difficult. As an alternative, consideration could be given to contracting with professional security consultants to carry out the necessary reviews.

Assessment of Cause
As noted in your report, the sophisticated nature of computer security reviews is beyond the expertise of the Office of Safeguard at this time. We have identified nine platforms already in use among the states. Each of these requires a specific degree of technical expertise in order to conduct a complete review. We do not have this expertise.

Corrective Action
We agree in concept that GLD needs to address this issue. As a result, we are currently conducting a study to look at the various alternatives, including the two mentioned in your recommendation--hire additional staff or contract with professional security consultants. In addition we are looking into the feasibility of self-certification and conducting joint audits with other federal agency reviewers. Finally, we are performing risk assessment studies so that our future reviews focus on the areas of greatest risk.

Implementation Date
Proposed Date: December 31, 2003

Responsible Official
Deputy Director, Governmental Liaison and Disclosure

Again, we appreciate the recommendations provided by the TIGTA team. If you have any questions, please contact Tom Marusin, Deputy Director of Government Liaison and Disclosure at (202) 622-6200.